Re: How do I choose constants suitable for Diffe-Hellman?

- *To*: ghio@chaos.bsu.edu (Matthew Ghio)
- *Subject*: Re: How do I choose constants suitable for Diffe-Hellman?
- *From*: M.Gream@uts.EDU.AU (Matthew Gream)
- *Date*: Tue, 6 Sep 94 8:53:21 EST
- *Cc*: cypherpunks@toad.com (Cypherpunks Mailing List)
- *In-Reply-To*: <199409051528.KAA07031@chaos.bsu.edu>; from "Matthew Ghio" at Sep 5, 94 10:28:26 am
- *Organization*: University of Technology, Sydney.
- *Sender*: owner-cypherpunks@toad.com

```
"Matthew Ghio" wrote:

> Yes, Phil Karn posted a list of such numbers to the list last May, and
> the program used to generate them.  Since some people have expressed
> their distaste for large files re-posted/forwarded to the list, I won't
> send it, but you can get it from ftp cs.cmu.edu:
> /afs/andrew.cmu.edu/usr12/mg5n/public/Karn.DH.generator

I needed a few of these primes a while ago, so I took a few minutes and
hacked Phil's code to operate distributed (ie. a central machine
carried out the sieving and handed off candidates to a set of other
machines to do the Rabin-Miller). With one Sun Sparc 690MP and approx
40 Sun Sparc LX's, it was getting results like:

acacia: 7:21pm  up  2:05,  20 users,  load average: 0.95, 0.98, 0.77
mg.{~/static/d/dist} date;./go;date
Sun Jul 24 19:21:57 EST 1994
[..]
  server calls:   7235
found modulus p =
72a925f760b2f954ed287f1b0953f3e6aef92e456172f9fe86fdd8822241b9c9788fbc289982743efbcc
finding generator
trying 2 3 5
generator g = 5
Sun Jul 24 21:10:18 EST 1994

That's 2 hours for a 2048 prime P where (P - 1)/2 is also prime, and they
also satisfied the constraint that P = 3(mod 4).

The software maintains a TCP connection to each "Rabin-Miller server"
and can dynamically deal with the loss of machines, but in it's
simplicity doesn't do reconnects.  If anyone who operates an FTP
archive wants to reply to me, I'll tar it up (in it's current "it works
for me, but no guarantees" state).

Speaking of primes with constraints, I got my hands on Harn's recent
paper on a PKCS based on both factoring and discrete logs. He wants his
modulus to be a prime P = 2p x q + 1, where p = 2r + 1, q = 2s + 1. All
P, q, q, r, s must be prime -- good luck in finding such primes by
probablistic methods !

Matthew.

mg.{~/src/rr} ls -l
```

```
total 26
-rw-------  1 mgream       8339 Jul 24 14:17 client.c
-rw-------  1 mgream       2196 Jul 24 15:00 common.h
-rw-------  1 mgream       6028 Jul 29 13:35 dhgen.c
-rwx------  1 mgream        270 Jul 24 14:58 go
-rw-------  1 mgream        527 Jul 24 14:58 makefile
-rw-------  1 mgream       3041 Jul 29 14:50 server.c
-rw-------  1 mgream        367 Jul 24 14:26 servers.src

--
Matthew Gream <M.Gream@uts.edu.au> -- Consent Technologies, (02) 821-2043
Disclaimer: From? \notin speaking_for(Organization?)            [cfqx103]
```

- **References**:
  - **Re: How do I choose constants suitable for Diffe-Hellman?**
    - *From:* Matthew Ghio <ghio@chaos.bsu.edu>

- Prev by Date: **Re: Art Gallery on internet needs PGP signatures**
- Next by Date: **PRIVACY 101**
- Prev by thread: **Re: How do I choose constants suitable for Diffe-Hellman?**
- Next by thread: **Re: Program to circumvent the Sep 1 Legal Kludge part 1/5**
- Index(es):
  - **Date**
  - **Thread**